SSA-148078: Multiple Vulnerabilities in APOGEE/TALON Field Panels

Publication Date: 2017-10-12
Last Update: 2022-06-14
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

Multiple vulnerabilities in the APOGEE PXC and TALON TC series of products could allow unauthenticated attackers to download sensitive information through the integrated webserver.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
APOGEE PXC Compact (BACnet): All versions < V3.5	Update to V3.5 or later version https://partnerportal.extranet.dc.siemens.com/ See further recommendations from section Workarounds and Mitigations
APOGEE PXC Compact (P2 Ethernet): All versions	Currently no fix is planned Disable the integrated webserver See further recommendations from section Workarounds and Mitigations
APOGEE PXC Modular (BACnet): All versions < V3.5	Update to V3.5 or later version https://partnerportal.extranet.dc.siemens.com/ See further recommendations from section Workarounds and Mitigations
APOGEE PXC Modular (P2 Ethernet): All versions	Currently no fix is planned Disable the integrated webserver See further recommendations from section Workarounds and Mitigations
TALON TC Compact (BACnet): All versions < V3.5	Update to V3.5 or later version https://partnerportal.extranet.dc.siemens.com/ See further recommendations from section Workarounds and Mitigations
TALON TC Modular (BACnet): All versions < V3.5	Update to V3.5 or later version https://partnerportal.extranet.dc.siemens.com/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Siemens recommends to disable the integrated webserver when not in use
- Please contact your local Siemens office for additional support

Product specific remediations or mitigations can be found in the section Affected Products and Solution.

Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

The APOGEE PXC Modular and Compact Series are high-performance Direct Digital Control (DDC) devices and an integral part of the APOGEE Automation System.

The TALON TC Modular and Compact Series are high-performance Direct Digital Control (DDC) devices and an integral part of the TALON Automation System.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2017-9946

An attacker with network access to the integrated web server (80/tcp and 443/tcp) could bypass the authentication and download sensitive information from the device.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2017-9947

A directory traversal vulnerability could allow a remote attacker with network access to the integrated web server (80/tcp and 443/tcp) to obtain information on the structure of the file system of the affected devices.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- RoseSecurity for reporting the vulnerabilities for APOGEE PXC Series (P2 Ethernet) devices.

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2017-10-12): Publication Date
V1.1 (2022-06-14): Added APOGEE PXC Series (P2 Ethernet) devices

TERMS OF USE